REMARKS

The Office Action dated May 9, 2006, has been received and carefully noted. The period for response having been duly extended from August 9, 2006, to October 9, 2006, by the attached Petition for Extension of Time, the above amendments to the claims, and the following remarks, are submitted as a full and complete response thereto.

Claims 1, 31 and 40 have been amended to particularly point out and distinctly claim the subject matter which is the invention. No new matter has been added, and no new issues are raised which require further consideration and/or search. Claims 3, 4, 33, 34, 42 and 43 have been cancelled Claims 1, 2, 5-32, 35-41 and 44-48 are submitted for consideration.

Applicant's representative wishes to thank the Examiner for the courtesy telephone call made by the Examiner in April 2006 to inform Applicants that claims 4, 34 and 43 include allowable subject matter. As noted during the telephone call, the Examiner indicated that claims 4, 34 and 43 included allowable subject matter. As noted below, claims 1, 31 and 40 have been amended to include the elements of claims 4, 34 and 43 respectively.

Claims 1-48 were rejected under 35 U.S.C. § 102(e) as allegedly being anticipated by U.S. Patent Publication No. 2002/0174335 to Zhang in view of U.S. Patent Publication No. 2003/0226017 to Palekar. According to the Office Action, Zhang teaches all of the elements of claims 1-48 except for establishing a secure tunnel based on

a protocol or an authentication method. Thus, the Office Action combined the teachings of Zhang and Palekar to yield all of the elements of claims 1-48. The rejection is traversed as being based on a reference that neither teaches nor suggests the novel combination of features clearly recited in independent claims 1, 31 and 40.

Claim 1, upon which claims 2-30 depend, recites in a communication system including at least one network, including network entities which provide connectivity to user equipment, a method of connecting the user equipment to the at least one network includes establishing a secure tunnel which provides connection between the user equipment and one of the network entities. The method also includes authenticating the user equipment with another of the network entities. The authenticating of the user equipment with another of the network entities occurs at least partially simultaneously with a phase of the establishing of the secure tunnel, wherein the phase is determined based on a protocol or authentication method. Establishing the secure tunnel begins before authenticating the user. During a time between a beginning of establishing the secure tunnel with one of the network entities and a beginning of authenticating the user equipment with another of the network entities, the at least one network communicates with the user equipment to confirm that the request from the user equipment to establish a secure tunnel is not part of a denial of service attack.

Claim 31, upon which claims 32-39 depend, recites a communication system including at least one network, including network entities which provide connectivity to the user equipment. A secure tunnel is established which provides connection between

the user equipment and one of the network entities. The user equipment is authenticated with another of the network entities. The authenticating of the user equipment with another of the network entities occurs at least partially simultaneously with a phase of the establishing of the secure tunnel. The phase is determined based on protocol or authentication method. secure tunnel, wherein the phase is determined based on a protocol or authentication method. Establishing the secure tunnel begins before authenticating the user. During a time between a beginning of establishing the secure tunnel with one of the network entities and a beginning of authenticating the user equipment with another of the network entities, the at least one network communicates with the user equipment to confirm that the request from the user equipment to establish a secure tunnel is not part of a denial of service attack.

Claim 40, upon which claims 41-48 depend, recites a user equipment in a communication system including at least one network, including network entities which provide connectivity to the user equipment. A secure tunnel is established which provides connection between the user equipment and one of the network entities. The user equipment is authenticated with another of the network entities, and the authenticating of the user equipment with another of the network entities occurs at least partially simultaneously with a phase of the establishing of the secure tunnel, wherein the phase is determined based on a protocol or authentication method. secure tunnel, wherein the phase is determined based on a protocol or authentication method. Establishing the secure tunnel begins before authenticating the user. During a time between a beginning

of establishing the secure tunnel with one of the network entities and a beginning of authenticating the user equipment with another of the network entities, the at least one network communicates with the user equipment to confirm that the request from the user equipment to establish a secure tunnel is not part of a denial of service attack.

As will be discussed below, the cited prior art references of Zhang and Palekar fail to disclose or suggest the elements of any of the presently pending claims.

Zhang et al. relates to an IP-based authentication, accounting and authorization scheme for wireless local area network (LAN) virtual operators. Zhang et al. describes mobile users accessing the internet and local network services at hot spots, such as airports, hotels or coffee shops. The internet service providers of the mobile users are used as the single point of contact for all authentication, accounting and authorization (AAA) transactions. Referring to Figure 1 of Zhang et al., a mobile terminal 110 communicates with a wireless LAN access point 120. Zhang et al. describes access point 120 controlling the authentication by mobile terminal 110. Figure 2 of Zhang et al. shows access point 120 assigning mobile terminal 110 a dynamic IP address. The user initiates a login session with the ISP. The ISP id and the user id are sent to access point 120. Access point 120 sends the user's authentication server an access-request packet 210 with the user id. RSP 150' makes a validity determination with respect to the user id contained in the access-request packet 210. Zhang et al. describes a filtering function installed on every access point 120 to filter all mobile traffic and determine whether the traffic should be let through or blocked. IPSEC is used between access points and mobile

terminals for per-packet authentication or per-packet encryption. A packet filtering function employed at an access point serves as a transparent mechanism for controlling not only authentication and authorization, but also packet level accounting. With a mutual proof mechanism, Zhang et al. describes avoiding potential accounting disputes without requiring all mobile traffic to go through a central entity.

Palekar discloses that a Transport Layer Security (TLS) protocol provides a mechanism for encrypting messages between two end points. The messages protected with the TLS protocol are to be transmitted through a TLS tunnel that was previously established. See at least paragraph 0008 of Palekar.

Applicant submits that the combination of Zhang and Palekar fails to teach or suggest each element of the presently pending claims. Claims 1, 31 and 40 recite, in part, establishing the secure tunnel begins before authenticating the user and wherein during a time between a beginning of establishing the secure tunnel with one of the network entities and a beginning of authenticating the user equipment with another of the network entities, the at least one network communicates with the user equipment to confirm that the request from the user equipment to establish a secure tunnel is not part of a denial of service attack.

As noted in the courtesy telephone call from the Examiner previously, dependent claims 4, 34 and 43 included allowable subject matter which is now recited in claims 1, 31 and 40. Zhang fails to disclose or suggest establishing the secure tunnel begins before authenticating the user and wherein during a time between a beginning of establishing the

secure tunnel with one of the network entities and a beginning of authenticating the user equipment with another of the network entities, the at least one network communicates with the user equipment to confirm that the request from the user equipment to establish a secure tunnel is not part of a denial of service attack, as recited in claims 1, 31 and 40.

Palekar does not cure any of the deficiencies of Zhang. Palekar does not include the allowable subject matter indicated by the Examiner. Specifically, Palekar does not teach or suggest establishing the secure tunnel begins before authenticating the user and wherein during a time between a beginning of establishing the secure tunnel with one of the network entities and a beginning of authenticating the user equipment with another of the network entities, the at least one network communicates with the user equipment to confirm that the request from the user equipment to establish a secure tunnel is not part of a denial of service attack, as recited in claims 1, 31 and 40. Thus, Applicant respectfully asserts that the rejection under 35 U.S.C. §103(a) should be withdrawn because neither Zhang nor Palekar, whether taken singly or combined, teaches or suggests each feature of claims 1, 31 and 40 and hence, dependent claims 2-30, 32-39 and 41-48 thereon.

As noted previously, claims 1, 2, 5-32, 35-41 and 44-48 recite subject matter which is neither disclosed nor suggested in the prior art references cited in the Office Action. It is therefore respectfully requested that all of claims 1, 2, 5-32, 35-41 and 44-48 be allowed and this application passed to issue.

If for any reason the Examiner determines that the application is not now in condition for allowance, it is respectfully requested that the Examiner contact, by

telephone, the applicants undersigned attorney at the indicated telephone number to arrange for an interview to expedite the disposition of this application.

In the event this paper is not being timely filed, the applicant respectfully petitions for an appropriate extension of time. Any fees for such an extension together with any additional fees may be charged to Counsel's Deposit Account 50-2222.

Respectfully submitted,

Arlene P. Neal
Registration No. 43,828

Customer No. 32294
SQUIRE, SANDERS & DEMPSEY LLP
14TH Floor
8000 Towers Crescent Drive
Tysons Corner, Virginia 22182-2700
Telephone: 703-720-7800
Fax: 703-720-7802

APN:kmp

Enclosures: Petition for Extension of Time
Check No. 15160